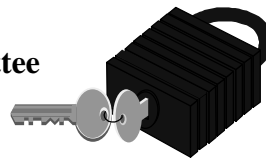


Federal Agency PKI Overview/KMS

Richard Guida, P.E.

**Member, Government Information
Technology Services Board**

Chair, Federal PKI Steering Committee



Richard.Guida@cio.treas.gov; 202-622-1552

<http://gits-sec.treas.gov>

Government Perspective on Key Management Standards

- * Government supports standards which:
 - *Are open in nature (non-proprietary)
 - *Promote interoperability of PKI products and clients
 - *Fully implement X509 certificate path discovery and processing including policy mapping
 - *Support two key pairs - signature, encryption
 - *Support encryption key recovery (business reasons)
 - *Contain appropriate specificity so as to be unambiguous and clear to implementers

Government Perspective on Key Management Standards (continued)

- * State of standards today is:
 - * Generally sufficient to support single product use within an enterprise
 - * Problematic when trying to make different products interoperate
 - * Many competing varieties in critical areas (e.g. CMP vs. PKCS)
 - * Inconsistent and incompatible implementations even with single standard

Environments in which encryption is needed are diverse

- * Intra-agency
 - personnel matters, agency management
- * Interagency
 - payments, account reconciliation, litigation
- * Agency to trading partner
 - procurement, regulation
- * Agency to the public

Current agency use of encryption is very limited

- * Many PKI implementations among Federal agencies, but all use digital signatures
 - *SSL planned for encryption
- * Agencies planning to use end-user PKI encryption in near term include:
 - *Federal Aviation Administration (FAA)
 - *Social Security Administration (SSA)
 - *Department of Defense (already done w/Fortezza)
 - *US Patent and Trademark Office

Interoperability Issues

- * **Policy interoperability**
- * **Technical interoperability**
- * **Interoperability among:**
 - * PKI products (CAs, RAs)
 - * Directories
 - * Client software (e.g., e-mail)
 - * Hardware tokens, devices, drivers

Encryption Key Recovery

- * KRDP Phase I very successful
- * KRDP Phase II is underway
 - * FAA
 - * SSA
 - * State Department
 - * Federal Bridge CA (interoperability)
- * Key recovery essential for business reasons

Federal PKI Approach

- **Establish Federal PKI Policy Authority (for policy interoperability)**
- **Implement Federal Bridge CA using COTS (for technical interoperability)**
- **Deal with directory issues in parallel**
 - Border directory concept
 - Use ACES for public transactions

Federal PKI Policy Authority

- **Voluntary interagency group - NOT an “agency”**
- **Governing body for interoperability through FBCA**
 - **Agency/FBCA certificate policy mappings**
- **Oversees operation of FBCA, authorizes issuance of FBCA certificates**

Federal Bridge CA

- **Non-hierarchical hub (“peer to peer”)**
- **Maps levels of assurance in disparate certificate policies (“policyMapping”)**
- **Ultimate bridge to CAs external to Federal government**
- **Directory initially contains only FBCA-issued certificates and ARLs**

Boundary Conditions

- **Use COTS with “inclusive” architecture**
- **Use X509v3**
- **Support four levels of assurance**
 - **Rudimentary, Basic, Medium, High**
 - **Modeled after Canadian PKI**
- **FBCA use cannot be mandatory**
- **Focus requirements on agencies as certificate issuers, not relying parties**

FBCA Architecture

- **Multiple CAs inside membrane, cross certified**
 - **Adding CAs straightforward albeit not necessarily easy**
- **Solves inter-product interoperability issues within membrane - which is good**
- **Single consolidated X.500 directory**

Current Status

- **Prototype FBCA: Entrust, Cybertrust**
 - Initial operation 2/00
- **Production FBCA: add other CAs**
 - Operation by late 00
- **FBCA Operational Authority is GSA**
(Mitretek technical lead and host site)
- **FBCA Cert Policy 12/99 to early 00**
- **FPKIPA Charter 12/99 to early 00**

Border Directory Concept

- **Each agency would have Border Directory for certificates and CRLs**
 - May shadow all or part of local directory system (allows for agency discretion)
 - CAs may publish directly in border directory
 - Unrestricted read access
- **Directory resides outside agency firewall**
 - chain (X.500 DSP) or LDAP referral to FBCA DSA

Border Directory Concept

The diagram illustrates the Border Directory Concept, showing three agencies (Agency 1, Agency 2, Agency 3) and their connections to a central FBCA (Federated Border Control Authority) and FBCA DSA (Federated Border Control Authority Directory Service).

Agency 1 (Left): Contains PCA 1 (Principal Control Agent) and is connected to Border DSA 1 (LDAP Server). A thick arrow points from PCA 1 to Border DSA 1.

Agency 2 (Right): Contains PCA 2 (Principal Control Agent) and is connected to Border DSA 2 (X.509 DSA). A thick arrow points from PCA 2 to Border DSA 2.

Agency 3 (Top Center): Contains PCA 3 (Principal Control Agent) and is connected to the FBCA. A thick arrow points from PCA 3 to the FBCA.

Central Components:

- FBCA:** Federated Border Control Authority, represented by a black oval.
- FBCA DSA:** Federated Border Control Authority Directory Service, represented by a grey rectangle.
- Border DSA 1 (LDAP Server):** Represented by a black oval.
- Border DSA 2 (X.509 DSA):** Represented by a black oval.

Connections:

- PCA 1 is connected to the FBCA and Border DSA 1.
- PCA 2 is connected to the FBCA and Border DSA 2.
- PCA 3 is connected to the FBCA.
- The FBCA is connected to the FBCA DSA.
- The FBCA DSA is connected to Border DSA 1 (LDAP Server) and Border DSA 2 (X.509 DSA).
- Border DSA 1 is connected to Border DSA 2.

Access Certs for Electronic Services

- **“No-cost” certificates for the public**
- **For business with Federal agencies only (but agencies may allow other uses on case basis)**
- **On-line registration, vetting with legacy data; information protected under Privacy Act**
- **Regular mail one-time PIN to get certificate**
- **Agencies billed per-use and/or per-certificate**

- **“No-cost” certificates for the public**
- **For business with Federal agencies only (but agencies may allow other uses on case basis)**
- **On-line registration, vetting with legacy data; information protected under Privacy Act**
- **Regular mail one-time PIN to get certificate**
- **Agencies billed per-use and/or per-certificate**

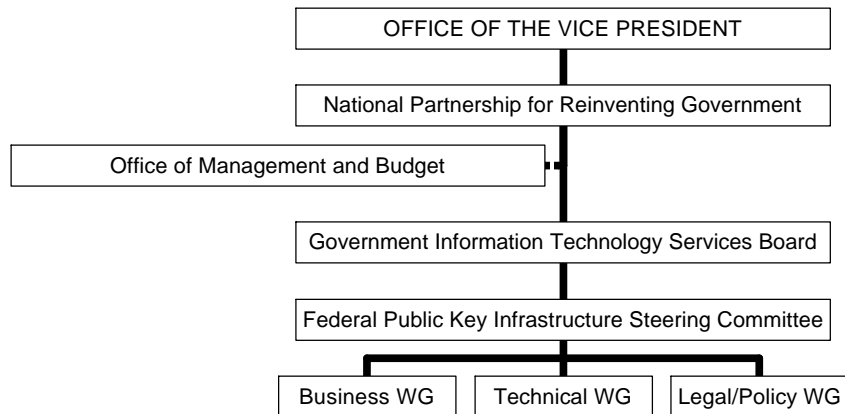
Access Certs for Electronic Services

- **RFP 1/99; bids received 4/99; first award 9/99 (DST), second award 10/99 (ORC), third award 10/99 (AT&T)**
- **Provisions for ACES-enabling applications, and developing customized PKIs**
- **Agencies do interagency agreement with GSA**
- **Certificates available shortly**

Electronic Signatures under GPEA

- **Government Paperwork Elimination Act (October 1998)**
- **Technology neutral - agencies select based on specifics of applications (e.g., risk)**
 - **But full recognition of dig sig strengths**
- **Gives electronic signature full legal effect**
- **Focus: transactions with Federal agencies**
- **Draft OMB Guidance 3/99; final 4/00**

Organization



Abbreviations

- ACES Access Certificates for Electronic Services
- ARL Authority Revocation List
- BCA Bridge CA
- CA Certificate Authority
- CMP Certificate Management Protocol
- COTS Commercial Off-the-Shelf
- CRL Certificate Revocation List
- DSA Directory System Agent
- DSP Directory Service Protocol
- DST Digital Signature Trust
- GSA General Services Administration
- FBCA Federal Bridge CA

Abbreviations (contd.)

- FPKIPA Federal PKI Policy Authority
- GPEA Government Paperwork Elimination Act
- KRDP Key Recovery Demonstration Project
- LDAP Lightweight Directory Access Protocol
- OMB Office of Management and Budget
- ORC Operational Research Corporation, Inc.
- PCA Principal CA
- PIN Personal Identification Number
- PKCS Public Key Cryptography Standard
- PKI Public Key Infrastructure
- RA Registration Authority
- RFP Request for Proposal